REMARKS:

Claims 1-3, and 5-20 are active in the application.

Claim 10 has been amended to specify that the system components are essential for device operation. This amendment is merely of a clarifying nature, and does not affect the scope of claim 10, or present any new issues.

Claims 1-9 and 18-20 were rejected under 35 USC 103(a) as being unpatentable over newly cited US Patent 6,321,335 to Chu. This rejection is traversed.

As noted in the prior response, claims 1 and 18 require writing an update code over an original security code in the fuses. The update code is necessarily an OR-function product of the original code and the update code. Contrary to incorrect statements in the Office Action, Chu does not in any way teach or suggest, or provide motivation for this feature. In fact, Chu teaches away from rewriting a new security code over the original code.

Chu does teach storing a security code in electronic fuses in cols. 9 and 10. However, the teaching in Col 9, lines 11-32 and col. 10 lines 65-67 relates to an embodiment in which the "code" is not an updatable security code or access password, but rather a permanent code that identifies the device (i.e. a "fingerprint"). In col. 9, lines 11-13, Chu states: "In still further embodiment, the present invention also includes a permanent password or user identification code to identify the computer module."

In col. 9, lines 15-22 Chu teaches that the code can be placed in the device "by a one time programming techniques (sic) using, for example, fuses or the like. The present password or user code provides a permanent fingerprint on the device". Hence, in the embodiment where Chu teaches the use of fuses, the code is permanent because it is used as a fingerprint. Fingerprints are not changeable or alterable in any way. In support of this, Chu specifically identifies fuses as a "one time programming technique". This is different from claims 1 and 18 which explicitly require changing the code. Chu, by contrast, is clear in asserting that fuses are for one-time programming to create unchangeable fingerprints.

In col. 9, lines 29-32, and col. 10, lines 65-67, Chu teaches that the permanent password or user code (i.e. the fingerprint) "can be combined with the password in flash memory for the security program, which is described below in more detail". Hence, Chu teaches that the "fingerprint" code used to identify the hardware (and which uses one-time programming techniques such as fuses), can be combined with erasable and rewritable techniques such as flash memory. Hence, the permanent fingerprint employing fuses is distinct from the rewritable aspects of Chu, which rely on flash memory.

In col. 8, lines 49-55, Chu teaches that the password "can readily be changed by erasing the code, which is stored in flash memory, and a new code (i.e. password° is written into the flash memory". Hence, Chu teaches that the password is necessarily erasable, which necessarily implies that it cannot employ fuses.

Chu in fact teaches away from modification (to program additional fuses and obtain an OR-function code) by explicitly stating (in col. 9 lines 18-20) that fuses comprise a one-time programming technique. Of course, blowing additional fuses to create an OR function product requires programming 2 or more times. Also, Chu teaches away from modification at col. 9, lines 29-32, which teach that the permanent "fingerprint" identification code, is distinct from and can be combined with a code stored on flash memory. Hence, the reprogrammability taught in col. 8, lines 50-55 applies to flash memory and other memory circuits, not to the "fingerprint" function associated with fuses in col. 9, lines 18-20.

The Office Action states that "Chu has the capability of updating a security code, by an OR function as well by blowing other fuses in addition to the already blown ones to create a new password". This is incorrect. This capability is not taught, suggested or motivated by Chu. Chu does not have the capability; this capability is new to Chu, and would require modification to the teachings of Chu. Also, the Office Action does not provide any prior art teaching, suggestion or motivation for modifying Chu to include overwriting of fuses. The supposed obviousness of the present claims is asserted without any justification in prior art or knowledge identified by the Examiner. It is based merely on the suggestion by the Examiner that modifying Chu according to the present invention to update codes programmed in fuses is possible and therefore obvious. This is not reasonable or supported by the prior art of record. A possibility of modification does not mean that modification is obvious. The Office Action is seemingly relying on the benefit of the present disclosure to assert that the capability of reprogramming fuses is obvious.

This hindsight is impermissible in an obviousness rejection. The combination claimed in claims 1 and 18 is unobvious to one of ordinary skill in the art because there is no teaching, suggestion, or motivation to make the modification, and, because in Chu there is a teaching away from the modification.

Also, it is important to note that Chu describes fuses in exactly two places: col. 9, lines 18-20, and col. 10, lines 65-67. In both places, Chu describes the fuses in exactly the same way: as one-time programmable devices which can be used to create a permanent fingerprint, which is contrary to the use of fuses in the present invention as claimed. Wholly absent from Chu is any teaching or suggestion that fuses can be overwritten or programmed a second time.

In view of the above arguments, it should be clear that Chu does not teach, suggest, or provide motivation for reprogramming fuses to obtain an OR function product used as a security code, as required by claims 1 and 18. Chu teaches away from this modification by differentiating between "fingerprint" code functions for fuses and reprogrammable functions for flash memory, and by consistently identifying fuses as one-time programmable devices used for "fingerprinting". The Office Action provides no justification for the obviousness of claims 1 and 18, other than to assert that the modification is obvious because it is possible. Accordingly, claims 1 and 18 are not obvious in view of Chu, and the rejections of these claims must be withdrawn.

Claim 10 was rejected under 35 USC 103(a) as being unpatentable over Chu in view of US Patent 6,687,843 to Kwak. This rejection is traversed.

Kwak teaches a memory circuit which reduces power consumption by "restricting generation of an unnecessary clock" (see col. 1, lines 10-13, col. 3, lines 29-31). In Kwak, it is essential to control the clock so that it is activated when the memory module containing the clock is addressed. The clock is activated when its address corresponds to a signal containing the address of the clock. In this way, a clock is turned on only when its address is identified in a signal. The clock of Kwak is not activated when it is not needed, thereby saving energy.

In Kwak, the signal used to activate the clock is a COLX or COLC packet indicating the address of the memory module that needs to be accessed. COLX packets and COLC packets are not security codes, and cannot function as security codes. Hence, this teaching of Kwak is very different from the present invention, and not combinable with Chu, as proposed in the Office Action.

The Office Action argues that Kwak teaches "comparing a signal to the address value and if it is a possible match, a clock enable signal is generated to enable the clock." As noted, Kwak uses COLC and COLX packets that indicate the memory module requested. Nowhere does Kwak teach or suggest that the signal can be a password or any other kind of user-input code. The "signal" in Kwak is an address that identifies the location in memory (i.e. the module) that must be accessed. The packets used by Kwak are therefore fundamentally different from the security codes used in the present invention.

Kwak does not teach or suggest that clock activation can be used to control access to a device, or that clock activation can be in response to a security code, as required in the present invention. In Kwak, disabling a clock merely reduces power consumption in the memory module associated with the clock. Disabling the clock of Kwak does not render the device inoperable, as required in claim 10.

Additionally, the clocks used in Kwak are not system clocks. System clocks provide clock signals for the system globally. Without the system clock, the system cannot operate. By comparison, the clock in Kwak is provided for use in specific memory modules. The clock of Kwak is not used by the system, and the clock is not essential for device operation, as required in claim 10.

In the present invention, the device is secured by comparing a password with the system security ID code in a comparator. The output of the comparator is used to enable/disable an essential system component, which is either a scan chain, PLL, or system clock. In this method, the device is secured <u>without software control</u>. Software-mediated access is inherently insecure, since viruses and hacking software can be used to change passwords and gain access. By comparison, the present invention relies exclusively on hardware to enable/disable the device. The exclusive reliance on hardware (e.g. the comparator in combination with scan chain, PLL, or system clock) in the present invention avoids the inherent risks associated with software security. The present hardware-based approach to authenticate passwords and enable/disable the device is inherently and absolutely impossible to hack using software techniques.

By comparison, Chu teaches that software is used to determine when a password is correct, and uses software to enable/disable the device. In Chu, software determines whether a match exists between stored and entered passwords, and software controls the disabling of the device. For example, col. 10, lines 1-6 teaches that a "security detection program" analyzes the password and controls the disabling of the device. A security detection program is not hardware, and absolutely has nothing to do with using a comparator to enable/disable an essential system component, as required by claim 10.

The Office Action includes several erroneous statements about the teachings of Chu and Kwak.

Firstly, the Office Action states: "Chu also states that access the access (sic) control can be electrical as it is in Kwak". This is misleading because Kwak does not teach any kind of "access control". Kwak is unrelated to computer security. Kwak merely turns on a clock when it is being addressed by a computer system. Chu teaches "electrical" control in the sense that software-based control is considered electrical. Chu does not teach that electrical hardware (e.g. a comparator in combination with a scan chain, PLL or clock as recited in claim 10) can be used to enable/disable the device. Chu relies on software; the present invention as claimed relies on hardware.

Secondly, the Office Action states: "Furthermore, Chu states that the software can turn a lock on which disables power unless the passwords match (figure 6), which demonstrates that the scan chains (hardware) can not be accessed unless the passwords match". This passage of the Office Action indicates that the present invention may have been misunderstood by the Examiner. In the present invention, scan chain disabling (or PLL or clock disabling) is the means for disabling the device. The fact that, in Chu, a scan chain may be disabled, or made inaccessible by software turning a lock, is irrelevant. The software-based security access of Chu is fundamentally different from the comparator-based enabling/disabling of essential system components. In Chu, software controls mechanical or electrical hardware to determine device access; in the present invention, electrical hardware control electrical hardware to determine device access. Software is not used at all in the present invention.

Thirdly, the Office Action states: "...it would have been obvious to use the clock disablement feature of Kwak conjuction (sic) with the system of Chu to reduce power consumption." Employing the teachings of Kwak to reduce power consumption in Chu will not produce the present invention as claimed. The present invention enables/disables the clock (or PLL or scan chain) based on password match or mismatch at the comparator, such that secure access is provided. The comparator enables/disables the essential system component (clock, PLL or scan chain). Controlling a clock in a memory module to minimize power consumption (required by Kwak) does not in any way provide secure access based on passwords, and will not provide enable/disable device control, as required in claim 10. Kwak is completely unrelated to password based secure access. The teachings of Kwak cannot be combined with the security aspects of Chu. So, while Kwak could possibly be used within the memory devices of Chu (e.g. within the flash memory) to reduce power consumption therein, Kwak could not be used within Chu to enable-disable a device based on passwords.

Nowhere do Chu or Kwak teach or suggest device access by entering a security code into a comparator to enable or disable an essential electrical hardware component such as a scan chain, phase lock loop, or system clock. Chu teaches software control; Kwak teaches enablement of a clock in a memory device based on which memory module is addressed. No possible combination of Chu or Kwak can produce the invention as claimed in claim 10 because both references lack a teaching or suggestion to use a security code-receiving comparator to enable/disable a scan chain, PLL, or clock for secure device access. Hence, the rejection of claim 10 must be withdrawn.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 1-3 and 5-20 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees for the petition or for entry of this amendment to IBM's Deposit Account No. 09-0458.

Respectfully submitted,

Michael E. Whitham
Reg. No. 32,635

Whitham, Curtis, & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA, 20190
Phone: 703-787-9400
Fax: 703-787-7557